BAB I

PENDAHULUAN

1.1. Latar Belakang

Perkembangan jaringan yang semakin pesat membuat para administrator dituntut untuk dapat bertanggung jawab pada manajemen perangkat jaringan dan dalam implementasinya bisa menjadi masalah karena dalam jaringan tradisional, tidak ada pemisahan antara *control plane* dan *data plane*. Setiap perangkat yang dikonfigurasi, diakses melalui CLI (*Command Line Interface*) [1]. Untuk mengatasi masalah tersebut, berkembanglah paradigma jaringan baru yang disebut dengan *Software Defined Network* (SDN). Jaringan SDN merupakan paradigma yang dibangun untuk mengatasi keterbatasan pada jaringan tradisional atau mengatasi masalah jaringan yang lebih rumit [2] [3], di mana pada jaringan ini *control plane* dan *data plane* dipisahkan menurut konsep dasarnya. *Control plane* bertanggung jawab atas konfigurasi jaringan sedangkan *data plane* yang menjalankan konfigurasi tersebut. Terdapat tiga layer pada arsitektur *Software Defined Network* (SDN), yaitu *data plane layer*, *control plane layer* dan *application layer* [4]. Data *plane layer* dan *control plane layer* dihubungkan dengan southbond interface (OpenFlow) sedangkan *control plane layer* dan *application layer* dihubungkan dengan northbond interface (API). Pada arsitektur SDN tidak menutup kemungkinan ancaman keamanan akan diterima. Salah satunya adalah serangan DDoS yang akan menyerang *controller* sehingga menyebabkan permasalahan pada *controller*. Beberapa metode untuk membebani *resource* pada *controller*, yaitu SYN Flood dan ICMP Flood [5].

Pada penelitian sebelumya, peneliti mendeteksi intrusi menggunakan honeypot untuk berinteraksi dengan *attacker* dan datanya akan dikumpulkan untuk dianalisis menggunakan dua tools, yaitu honeyd pada linux dan kfsensor pada windows. Parameter yang disimulasikan pada penelitian ini adalah TCP, UDP ICMP, FTP dan SSH. Pada honeyd berbagai IP terdeteksi di jaringan aman dan tidak aman sedangkan kfsensor menunjukan IP yang terdeteksi hanya pada jaringan

kfsensor dibangun [6]. Penelitian lainnya, menggunakan tipe serangan DDoS pada Cloud. Untuk mendeteksi dan mencegah serangan digabungkan dua metode, yaitu honeypot dan model NICE. Dimana, honeypot akan menjebak penyerang dan agen NICE memantau jaringan. Untuk memperbaharui basis data untuk berbagai serangan yang terjadi akan dilakukan oleh VM Profiller. Jenis serangan akan dianalisis menggunakan dua algoritma *Alert Correlation Graph* untuk serangan yang tidak diketahui dan *Honeypot Redirection and Countermeasure Selection*. Hasilnya akan dikirimkan notifikasi ke pengontrol jaringan lalu dilakukan mitigasi untuk serangan tersebut [7]. Penelitian sebelumnya, untuk mengatasi masalah terhadap ancaman keamanan pada wireless maka diusulkan metode Honeypot IDS. Metode gabungan ini akan mengurangi *false alarm rate*. Menggunakan tipe serangan MITM, DoS, DNS Spoofing dan ARP Poisoning. Pendekatan terdiri dari tiga fase, yaitu filter, sistem deteksi intruksi dan honeypot. Traffic akan dilewati untuk melakukan penyaringan dan deteksi. Setelah itu, diselidiki untuk setiap uji coba serangan dan hasilnya akan dianalisis [8]. Selain itu, terdapat penelitian yang telah menerapkan Honeypot dan SDN yang berjudul *HONEYPROXY: Design and Implementation of Next-Generation Honeynet via SDN* [9]. Dimana, penelitian ini merancang dan mengimplementasikan honeypot berbasis SDN untuk mencegah penyebaran *malware* di dalam jaringan dan mendukung adanya transisi honeypot dari *low-interaction* ke *high-interaction.*

Pada penelitian tentang *Intrusion detection using honeypots* deteksi disimulasikan pada jaringan biasa dengan lingkungan yang berbeda untuk masing-masing sensor yang diusulkan, yaitu honeyd dan kfsensor. Dari penelitian ini berhasil mendeteksi serangan yang masuk menggunakan *honeypot*, namun belum ada mitigasi yang dilakukan setelah terdeteksi adanya serangan [6]. Penelitian tentang *Attack Detection in Cloud Virtual Environment and Prevention Using Honeypot* dilakukan di jaringan virtual untuk melakukan pendeteksian serangan pada *Cloud* dan hasil yang diperoleh menunjukkan serangan terkadang tidak terdeteksi secara akurat dan *false alarm* juga dihasilkan [7]. Sedangkan penelitian [8] tentang *The Performance Analysis of Honeypot Based Intrusion Detection System for Wireless Network* mendeteksi serangan intrusi dilakukan pada jaringan wireless yang telah dibangun dengan menggunakan 6 komputer yang terdiri dari 1

penyerang, 4 *host* dan 1 komputer yang dipasang kfsensor serta 1 router. Hasilnya dari penelitian tersebut berhasil mengurangi *false alarm* tetapi belum ada mitigasi yang dilakukan.

Untuk itu, penelitian ini akan menerapkan sistem Honeypot Suricata dengan Modern Honey Network (MHN) menggunakan metode *entropy* untuk mendeteksi dan mitigasi serangan DDoS pada jaringan SDN. Honeypot suricata di MHN dapat digunakan untuk menjebak dan merekam aktivitas penyerang dengan tujuan mengumpulkan data serangan [10] [11]. Pada arsitektur ini, metode *entropy* akan menghitung tingkat keacakan paket yang masuk dan akan diklasifikasi apakah paket-paket yang masuk termasuk serangan atau tidak. Jika termasuk serangan, maka MHN yang bertindak sebagai *reactive preventive* akan menginstall flow mitigasi. Harapannya, penelitian ini dapat mendeteksi dan memitigasi serangan DDoS dengan baik.

1.2. Rumusan Masalah

Beberapa rumusan masalah yang dapat dimunculkan dari permasalahan di atas adalah sebagai berikut.

1. Apakah dapat menerapkan sistem honeypot suricata dengan MHN untuk deteksi DDoS tipe ICMP *flood* pada SDN menggunakan metode *entropy*?
2. Bagaimana hasil dari uji coba penerapan sistem honeypot suricata dengan MHN pada SDN menggunakan metode *entropy*?

1.3. Tujuan Penelitian

Berikut merupakan beberapa tujuan dari penelitian yang telah dilakukan antara lain.

1. Dapat menerapkan sistem honeypot suricata dengan MHN untuk deteksi DDoS tipe ICMP *flood* pada SDN menggunakan metode *entropy*.
2. Berhasil menganalisis hasil dari uji coba penerapan sistem honeypot suricata dengan MHN pada SDN menggunakan metode *entropy*.

1.4. Batasan Masalah

Adapun batasan masalah yang akan dicakup pada tugas akhir ini sebagai

berikut.

1. Arsitektur yang digunakan adalah SDN
2. Sistem operasi yang digunakan adalah *Ubuntu Desktop* 18.04 LTS
3. Jenis serangan yang akan digunakan adalah DDoS tipe ICMP Flood
4. Menjebak penyerang menggunakan honeypot suricata dan datanya akan dikumpulkan menggunakan MHN
5. Penelitian ini menggunakan metode *entropy* untuk menghitung keacakan jumlah paket yang masuk
6. *Controller* yang digunakan adalah *Ryu*
7. *Southbound* API adalah OpenFlow